ANTI-MONEY LAUNDERING:

THE CRIMINAL AND REGULATORY FRAMEWORK, AND ANTI-MONEY LAUNDERING COMPLIANCE PROGRAMS

By

GREG BALDWIN
Holland & Knight LLP
701 Brickell Ave, Suite 3000
Miami, Florida 33131

Tel: 305 789 7745
Fax: 305 789 7745
E Mail: gbaldwin@hklaw.com

1. WHAT IS MONEY LAUNDERING?

Money laundering is the general term used to describe the processes used to conceal the true source, origin, ownership, destination or use of money or property. It "is the criminal practice of processing ill-gotten gains, or 'dirty' money, through a series of transactions; in this way the funds are 'cleaned' so that they appear to be proceeds from legal activities."[1] The "dirty" money may have come from virtually any illegal activity, or it may be planned for an illicit purpose, like terrorism, but in every case it has one thing in common: to give money the appearance of having come from a legitimate source or being used for a legitimate purpose.

For the average criminal, money laundering is the process by which his or her criminal proceeds are made to look legitimate. For the average terrorist, money laundering is the process used to fund terrorist activity without revealing the true source, destination or purpose of the money. Money laundering provides the vehicle for criminals and terrorists to operate and expand their criminal enterprises. To do so, they must achieve one essential goal: they must exploit legitimate businesses. This is the only way they can accomplish their common goal of making their money and themselves look legitimate.

Many criminal activities (including, but certainly not limited to, drug dealing) generate enormous profits. Other criminal activities (including, but not limited to terrorist activity) require the secret movement of funds. Whether generated by criminal activity or planned for criminal use, these funds can only be used safely if the criminal or terrorist is able to place funds into the legitimate

[1] Federal Financial Institutions Examination Council, *Bank Secrecy Act – Anti-Money Laundering Examination Manual*," 2006, p. 7. Black's Law Dictionary, 8th ed., defines the term as "[t]he act of transferring illegally obtained money through legitimate people or accounts so that its original source cannot be traced."

financial system, efficiently and securely move them in order to cover their source, ownership or purpose, and then use them, all without attracting unwanted attention to the underlying criminal activity or purposes involved. Thus, money laundering is vital to the ultimate success of criminal and terrorist operations.[2]

2. HOW DOES MONEY LAUNDERING WORK?

The methods and means of laundering money are limited only by the imagination of the money launderer. Money launderers have one essential, common goal: to exploit legitimate financial institutions and businesses in such a way as to make their money and their activities look legitimate. Accordingly, they will do everything in their power to trick and deceive legitimate businesses. Although there are many different methods they may use, however, there are three generally recognized and independent steps that can often occur simultaneously:

> ***PLACEMENT*** – Most criminal activity generates cash. Large amounts of cash are hard to spend without attracting undesirable attention, are hard to move because of the bulk, and are hard to conceal. The only solution to these problems is to place the cash into the financial system, where it will be safer and much easier to move and conceal. The essential process of getting criminal cash into the financial system is known as the *"placement"* stage of money laundering.
>
> ***LAYERING*** – Once illicit funds have been placed gotten into the financial system, the money launderer needs to conceal them as completely as possible. To accomplish this, the money launderer moves the funds that have been placed in the financial system from business to business (often but not always phony businesses), country to country, and continent to continent. This creates a trail that is extremely difficult and time consuming for law enforcement to follow – which is the entire point of the effort. This process of moving the money through a complicated, extended trail in order to conceal its source, ownership or purpose is known as the *"layering"* stage of money laundering.
>
> ***INTEGRATION*** – Once illicit funds have been hidden through the layering process, the money launderer is ready to use the money. To accomplish this, the money launderer will seek ways to efficiently "resurface" the money so that it looks completely legitimate – such as from the legal sale of products, employment or consulting fees from apparently legitimate businesses, or the return on legal

[2] "Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes." *Id.,* p.8. ("Conflict diamonds" originate from areas controlled by factions opposed to legitimate governments and are used to finance military action in opposition to those governments. *See id.*)

investments. This process of making the illicit funds available so that they look "clean" is known as the *"integration"* stage of money laundering.[3]

In the placement stage the most common form for the funds to be in is cash. In the layering and integration stage, it most commonly involves monetary instruments (such as wire transfers) and other forms of property.

In light of these three essential steps, it is essential to understand that money laundering involves more than just cash transactions. Money laundering and terrorist financing can involve every possible form that money and property can take in addition to cash: money orders, checks, cashier's checks, bank drafts, wire transfers, traveler's checks, letters of credit, credit cards, life insurance annuities, real property, and so on. It can also involve products, like precious stones and metals, or jewelry.

3. WHAT IS THE ANTI-MONEY LAUNDERING LEGAL FRAMEWORK?

There are several key federal statutes that together constitute the U.S. government' efforts to detect and deter money laundering. Some apply only to certain types of businesses. Others apply to all businesses and all persons in the United States and, in some cases, even to persons and businesses located *outside* the United States.

The key laws are: (1) the Money Laundering Control Act; (2) the Bank Secrecy Act; (3) the federal laws requiring the reporting of large cash transactions; and (4) the federal laws prohibiting transactions with "specially designated" persons, such as narcotics trafficking "kingpins," terrorists and supporters of terrorist activity. There are also special laws regarding "Money Services Businesses" or "MSBs."[4]

In discussing these laws, it is important to keep in mind the general legal principle of "corporate liability." Under the law of the United States, every business is legally responsible for the acts or omissions of its employees and agents, as long as those employees or agents: (a) were acting within the scope of their employment; and (b) were acting for at least the partial benefit of their employer.

Thus, if the law requires some act to be performed and an employee purposely fails to perform that act because he or she thinks it may help the business, both that employee *and* the business can be criminally prosecuted for the failure to perform the act. Conversely, if the law prohibits some act and an employee performs that act anyway, then again, both that employee *and* the business itself can be criminally prosecuted for the associate's actions. Because of this general principle, it is of the utmost importance that every business and its employees at all time refrain from doing what the anti-money laundering laws prohibit, and scrupulously perform all acts that the anti-money laundering laws require.

---

[3] *See, e.g.*, Federal Financial Institutions Examination Council, *Bank Secrecy Act – Anti-Money Laundering Examination Manual*," 2006, p. 8.

[4] MSBs include: currency dealers or exchangers; check cashers; issuers or sellers of cashier's checks, traveler's checks, money orders, or stored value; and money transmitters. 31 C.F.R. 103.11(uu).

1. The Money Laundering Control Act

The Money Laundering Control Act consists of two criminal statutes, 18 U.S.C. §§ 1956 and 1957. Generally, the Act makes it a federal crime to launder money. Violation of this law can result in up to 20 years imprisonment for an individual and substantial fines for both an individual and a business.

Both sections of the Act apply to all persons and businesses in the United States. Prosecution under the Act can thus include not only the person responsible for the underlying crime that generated the illicit funds laundered, but also any person or business that knowingly assists or attempts to assist in the effort, or that is "willfully blind" to the source of the funds. In addition, certain provisions of the Act provide for extraterritorial jurisdiction, thus make it applicable to persons and businesses *outside* the United States.

As will be seen below, the Money Laundering Control Act is complicated and involves numerous elements. Stripped to its barest essentials, however, the Act generally provides that any person or business that "knows" that funds or property involved in "a financial transaction" come from "some unlawful activity," and then engages in or attempts to engage in the financial transaction involving those funds or property, or transports, transmits or transfers such funds or property, may have violated the Money Laundering Control Act if the funds or property come from or are intended to further a "specified unlawful activity."

Many of the terms used in the Money Laundering Control Act are specifically defined in the statute, and it is essential to understand those definitions in order to understand the scope of activity that can be considered criminal money laundering.

(a) Key Definitions for Sections 1956 and 1957:

(i) "Some Form of Unlawful Activity": "Some form of unlawful activity" means any activity that constitutes a felony under *any* federal law, *any* state law, or *any* law of a foreign country. A person may be wrong about what the actual illegal activity was, but knowledge of the true criminal source of the funds or property is irrelevant. All a person needs to know is that the funds or property has come from some illegal activity. The law provides that no person or entity may get involved with funds or property they know is "dirty" money; it does not say the person or entity involved needs to know where the "dirt" came from.[5]

(ii) "Knowledge": As interpreted by the case law, "knowing" the property comes from "some" form of illegal activity means not only *actual* knowledge that the funds came from some illegal activity, but also "deliberate indifference," or "willful blindness." The term "deliberate indifference" is defined as "the careful preservation of one's ignorance despite awareness of circumstances that would put a reasonable person on notice of a fact essential to a crime."[6] "Willful blindness" is the "deliberate avoidance of knowledge of a crime, especially by

[5] 18 U.S.C. § 1956(c)(1).

[6] Black's Law Dictionary, 8th Ed..

failing to make a reasonable inquiry about suspected wrongdoing despite being aware that it is highly probable."[7]

Willful blindness occurs in situations in which one is aware of facts that would cause a reasonable person's suspicions to be aroused, but further inquiry is deliberately omitted because one wishes to remain in ignorance of the true facts.[8] It is the intentional "cutting off of one's normal curiosity by an effort of the will."[9] A person may not escape criminal liability by pleading ignorance "if he … strongly suspects he is involved with criminal dealings but deliberately avoids learning more exact information about the nature or extent of those dealings."[10]

One may not turn a blind eye to the truth, or ignore "red flags" that indicate funds or property are derived from some unlawful activity, simply to avoid learning the truth. Putting one's head ostrich-like in the sand will not provide an excuse later on because one did not see anything. Willful blindness creates an inference of *actual* knowledge of the factual element in issue. If a jury concludes that a person deliberately ignored the warning signs or "red flags" that funds or property involved in a transaction were derived from some form of illegal activity, the law will permit that jury to infer that the person *actually knew* this the funds or property were criminally derived.

(iii) "Specified Unlawful Activity": Specified unlawful activities include both violations of approximately 250 federal criminal laws as well as violations of certain *foreign* laws. The particular federal criminal violations are listed in section 1956(c)(7). Specifically included are all acts listed as predicate acts in the federal RICO statute, 18 U.S.C. § 1961(1). As a result of the breadth of section 1956(c)(7) and the RICO list of predicate acts, virtually any federal criminal offense can be considered as a "specified unlawful activity."

The particular *foreign* laws that constitute "specified unlawful activity include: (1) violations of foreign drug laws; (2) crimes of violence, such as murder, kidnapping, extortion, and terrorism; (3) fraud by or against a foreign bank; (4) public corruption, such as bribery, misappropriation or embezzlement of public funds; (5) illegal arms dealing; (6) sexual exploitation of children and "trafficking in persons" in general; (6) any act for which the United States would be obligated to extradite for under a treaty with the nation in question.[11]

(iv) "Financial Transaction": A "financial transaction" is defined to include virtually every type of transaction that can be imagined. Specifically, the term covers: (1) a transaction that affects interstate or foreign commerce involving the movement of funds, monetary instruments or the transfer of title of any real property, vehicle, vessel or aircraft; and

---

[7] *Id.*

[8] *United States v. Murray*, 154 Fed. Appx. 740, 744, 2005 WL 3046549 (11th Cir. 2005).

[9] *United States v. Leahy*, 464 F.3d 773, 796 (7th Cir. 2006).

[10] *United States v. Craig*, 178 F.3d 891, 896 (7th Cir. 1999).

[11] 18 U.S.C. § 1956(c)(7)(B).

(2) a transaction involving the use of a financial institution engaged in, or whose activities affect, interstate commerce.[12]

(v) "Monetary Instruments": Monetary instruments are defined, for purposes of the Act, as "(i) coin or currency of the United States or any other country, traveler's checks, personal checks, bank checks and money orders, or (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery."[13]

(vi) "Financial Institution": As used in the Money Laundering Control Act, the term "financial institution" means much more than just banks, although banks (including *foreign* banks as defined in 12 U.S.C. 3101) are certainly included. The term also includes all businesses listed as "financial institutions" under the Bank Secrecy Act, 31 U.S.C. § 5312(a)(2), thus extending the meaning to include a host of other businesses as well.[14]

(b) 18 U.S.C. § 1956: Section 1956 (entitled "Laundering of Monetary Instruments") criminalizes three types of activity which can generally be described as "transaction money laundering," transportation money laundering," and "sting operations.".

(i) "Transaction Money Laundering" -- Conducting Certain Types of Financial Transactions: The Act prohibits any person or entity from engaging or attempting to engage in a "financial transaction,"

* "knowing" that the property involved in the transaction represents the proceeds of "some form of unlawful activity," and with

** (A) the intent to promote a "specified unlawful activity" or 26 U.S.C. § 7201 (tax evasion) or 7206 (fraud and false statements on a tax return or related documents), or

** (B) knowing that the transaction is at least partly designed to conceal the true nature, location, source, ownership or control of the proceeds of a "specified unlawful activity"

* if the funds or property are in fact derived from a specified unlawful activity.[15]

(ii) "Transportation Money Laundering" -- Moving Certain Funds or Monetary Instruments: The Act prohibits any person or entity from transporting, transmitting or transferring, or attempting to do so, any "funds" or "monetary instrument" into, out of or through the United States,

* with the intent to promote a "specified unlawful activity," or

---

[12] 18 U.S.C. §§ 1956(c)(3) and (4).

[13] 18 U.S.C. § 1956(c)(5).

[14] 18 U.S.C. § 1956(c)(6). *See* Section 3.3(a), p. 9, below, for a list of Bank Secrecy Act "financial institutions."

[15] 18 U.S.C. § 1956(a)(1).

* knowing that the funds or instrument represent the proceeds of some form of unlawful activity, and also

* knowing that the movement is designed at least in part to either

(A) conceal the true nature, location, source, ownership or control of the proceeds of a "specified unlawful activity" or

(B) avoid a federal or state transaction reporting requirement.[16]

(iii) "Sting Operations": The Act prohibits any person or entity that conducts or attempts to conduct a "financial transaction" involving property "represented to be" the proceeds of a "specified unlawful activity," or property used to conduct or facilitate a "specified unlawful activity" with the intent to:

* promote the "specified unlawful activity," or

* conceal the true nature, location, source, ownership or control of the proceeds of the "specified unlawful activity," or

***** avoid a federal or state transaction reporting requirement.[17]

The phrase "represented to be" means any representation made by a law enforcement officer or another person at the direction or with the approval of a Federal law enforcement officer. Thus, funds in an undercover "sting" operation can be considered to be the proceeds of a "specified unlawful activity" even if they are *not* derived from such activity, but an undercover agent *says* they are.

(iv) Penalties:

(a) Criminal: Any person or entity convicted of violating Section 1956 may be sentenced to twenty years in prison and/or a criminal fine of $500,000 or twice the value of the property, whichever is *greater.*[18]

(b) Civil: Sections 1956(a)(1), (a)(2) and (3) may also be enforced by civil penalty in the amount of $10,000 or twice the value of the property, whichever is *greater.*[19]

---

[16] *See, e.g.,* Section 3.3, at pp. 12-14, below. 18 U.S.C. § 1956(a)(2). In addition, for purposes of section (a)(2), a defendant's knowledge can be established if: (i) a law enforcement agent states that the funds or monetary instruments represent the proceeds of "some form of unlawful activity;" and (ii) the defendant's subsequent statements or actions indicate that the defendant believed this to be true.

[17] 18 U.S.C. § 1956(a)(3).

[18] 18 U.S.C. § 1956(a).

[19] 18 U.S.C. § 1956(b)(1).

(c) Forfeiture: Any real or personal property involved in a transaction or attempted transaction in violation 2of section 1956, or any property traceable to such property, is subject to civil or criminal forfeiture by the United States.[20]

However, "tracing" the property to the offense is *not* required under two circumstances. First, if funds subject to forfeiture are deposited at a foreign bank, and that foreign bank has an "interbank account" with a U.S. bank, a branch or agency of a foreign bank in the U.S., or a broker or dealer registered with the SEC. In such cases, funds may be seized directly from the "interbank account" and neither the foreign bank nor the U.S. entity holding the "interbank account" has standing to contest the forfeiture.[21]

The second instance in which "tracing" is not required is in a civil forfeiture action in which the subject property consists of cash or monetary instruments in bearer form deposited into a financial institution, if the forfeiture action is commenced within one year of the offense that is the basis for the forfeiture.[22]

(v) Extraterritorial Jurisdiction: Section 1956 applies not only to persons and entities inside the United States, but also, under certain circumstances, to persons and entities located *outside* the U.S. The Act confers jurisdiction over conduct that occurs in foreign countries and conduct by a foreign person or foreign "financial institution" if

* the conduct is by a U.S. citizen; or

* the conduct is by a non-United States citizen and occurs at least in part in the United States; and

* the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.

In addition, the federal courts have jurisdiction over foreign persons and entities for the propose of imposing the civil penalties for a violation of §§ 1956(a)(1), (a)(2) or (a)(3) when the foreign person or entity

* commits one of the three offenses involving a financial transaction that occurs in whole or in part in the United States;

* converts to his, her or its own use property that has been forfeited to the United States by court order; or

[20] 18 U.S.C. § 981(a)(1).

[21] 18 U.S.C. § 981(k). An "interbank account" means any account held by a foreign bank in the United States primarily for the purpose of facilitating customer transactions. *See* 18 U.S.C. §§ 981(k)(4)(a) and 984(c)(2)(B).

[22] 18 U.S.C. § 984.

***** the foreign person is a "financial institution" that maintains a bank account at a financial institution in the United States.[23]

The term "financial institution" is includes any of the several dozen types of businesses defined as such in the Bank Secrecy Act (31 U.S.C. § 5312(a)(2)), or any foreign bank.[24] For purposes of enforcing section 1956(a), a U.S. court may issue a restraining order to ensure that any bank account or other property held in the United States by a defendant is available to satisfy a judgment. The courts have the authority to appoint a Federal Receiver to find and collect all of a defendant's assets, wherever located, to satisfy a civil or criminal judgment, or an order of forfeiture. The Federal Receiver is granted substantial powers to accomplish this task.[25]

(c) 18 U.S.C. § 1957: Section 1957 (entitled "Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity") makes it illegal for any person or entity to knowingly engage or attempt to engage in a "monetary transaction" in "criminally derived property" of a value over $10,000, if the property is, in fact, derived from a "specified unlawful activity." The definitions applicable to section 1956 apply also to section 1957.

A "monetary transaction" means the deposit, withdrawal, transfer or exchange of funds or monetary instruments by, through or to a "financial institution."[26] Since "financial institution" includes the broad array of businesses included under this term in the Bank Secrecy Act, the Act essentially makes it illegal to *spend* any funds derived from a "specified unlawful activity" without regard for the intent or purpose of the transaction.

Further, the government need not prove that the defendant knew that the offence from which the funds were derived was a "specified unlawful activity." It is enough for the defendant to know only that the funds were "criminally derived." Thus, and "financial institution" which *receives* funds in a transaction and knows, or is willfully blind" to the fact, that the funds come from criminal activity, can be held to have violated section 1957.

"Criminally derived property" means any property, in whatever form, constituting or derived from proceeds obtained from a criminal offense.[27]

A "specified unlawful activity" has the same meaning as that used for purposes of 1956.[28]

Similar to section 1956, this section also confers extraterritorial jurisdiction on the government to prosecute offenses. Under section 1957, an offense occurring *outside* the United States may be prosecuted if the defendant is a "United States Person." A "United States Person"

---

[23] 18 U.S.C. § 1956(b(2).

[24] 18 U.S.C. § 1956(c)(6). The "financial institutions" included in the Bank Secrecy Act are listed in Section 3.2(a) at p. 9, below.

[25] 18 U.S.C. §§ 1956(b)(2) through (4).

[26] 18 U.S.C. § 1957(f). The term specifically excludes, however, paying an attorney for representation in a criminal matter.

[27] 18 U.S.C. § 1957(f)(2).

[28] 18 U.S.C. § 1957(f)(3).

includes a national of the U.S., any resident alien, any person within the U.S., any entity composed principally of nationals or permanent resident aliens of the U.S., or any corporation organized under the laws of the U.S., any state, the District of Columbia, or any territory or possession of the U.S.[29]

Violations of section 1957 are punishable by imprisonment for up to ten years. In addition, the forfeiture provisions described above in Section 1.1(a)(iv) also apply to violations of section 1957.

2. The Bank Secrecy Act

The Bank Secrecy Act (or "BSA") (31 U.S.C. 5311 *et seq.*) is the law that establishes the basic *regulatory* framework for anti-money laundering regulations.[30] Unlike the Money Laundering Control Act, the BSA applies only to certain types of businesses. The types of businesses it applies to are further limited by the implementing regulations issued by the Secretary of the Treasury.

The BSA applies to businesses classified as "financial institutions," and authorizes the U.S. Treasury Department to require that certain anti-money laundering actions, including reporting of large cash (*i.e.*, over $10,000) transactions, making and keeping certain records, implementing a formal, written Anti-Money Laundering Compliance Program, and mandatory reporting of "suspicious activity" to the federal government.

(a) "Financial Institutions" Defined: The term "financial institution" means much more than banks. The term is defined in 31 U.S.C. 18 U.S.C. 5312(a)(2) and (c) to include: (1) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h)); (2) a commercial bank or trust company; (3) a private banker; (4) an agency or branch of a foreign bank in the United States; (5) any credit union; (6) a thrift institution; (7) a broker or dealer registered with the SEC under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq*;); (8) any futures commission merchant, commodity trading advisor, or commodity pool operator registered or required to be registered under the Commodity Exchange Act; (9) a broker or dealer in securities or commodities; (10) an investment banker or investment company; (11) "money services businesses" or "MSBs";[31] (13) an operator of a credit card system (14) an insurance company; (15) a dealer in precious metals, stones, or jewels; (16) a pawnbroker; (17) a loan or finance company; (18) a travel agency; (19) a money transmitter; (20) a telegraph company; (21) a business engaged in the sale of automobiles, airplanes, and boats; (22) persons

[29] 18 U.S.C. §§ 1957(d)(2) and 3077(2).

[30] However, the provisions of the BSA can also be enforced through criminal prosecution against individuals and businesses. A willful violation of the BSA or a regulation prescribed under the BSA is punishable by fine of up to $250,000 and imprisonment for up to five years. Such violations, if committed while violating another law of the United States or as part of a pattern of any illegal activity involving over $100,000 in a one year period are punishable by a fine of up to $500,000 and imprisonment for up to ten years. Violations of sections 5318(i) or (j) (relating to private banking and correspondent accounts), or any regulations or special measures imposed under section 5318(A), are punishable by a fine equal to not less than two times the amount of the transaction, but not more than $1 million. 18 U.S.C. § 5322.

[31] MSBs include: currency dealers or exchangers; check cashers; issuers or sellers of cashier's checks, traveler's checks, money orders, or stored value; and money transmitters. 31 C.F.R. 103.11(uu).

involved in real estate closings and settlements; (23) the U.S. Postal Service; (24) an agency of the U.S. government or of a state or local government carrying out a power or duty of a business described in section 5312; (25) a casino, a gambling casino, or gaming establishment with an annual gaming revenue of more than $1 million annually; (26) any business engaging in an activity the Secretary determines by regulation to be similar to, related to, or a substitute for any business described in section 5312; and (27) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

(b) Regulatory Implementation of the Bank Secrecy Act: The Secretary of the Treasury has issued regulations requiring the implementation of anti-money laundering programs only for *some* of the "financial institutions" listed in the Bank Secrecy Act, and has exempted others. All of the implementing regulations are found at 31 C.F.R. 103.

Currently, the "financial institutions" subject to specific implementing regulations are: all banks regulated by a federal regulatory agency; businesses regulated by the SEC; credit unions regulated by the National Credit Union Administration; mutual funds; "money services businesses;" operators of credit card systems; some dealers in precious metals, precious stones or jewels; and certain life insurance companies.[32] All other businesses that fall within the definition of "financial institution" have been exempted from the provisions of the BSA, at least for the time being.[33] A careful reading of the BSA regulations is important for all "financial institutions" because some types of businesses that fall within the general description (particularly line insurance companies and dealers in precious metals, stones or jewels) may be excluded from the regulatory definitions.[34]

(c) General Regulatory Requirements for Subject Financial Institutions: The basic anti-money laundering requirements that the BSA imposes on "financial institution" are: (i) implementing an Anti-Money Laundering Program; (ii) the implementation of "Customer Identification Programs ("CIP"); and (iii) the reporting of "suspicious transactions" to the Treasury Department. Not all of these requirements are equally applicable to subject "financial institutions," and accordingly careful review of the applicable regulations is necessary.

---

[32] *See* variously: 31 C.F.R. 103.120; 103.125; 103.130; 103.135; 103.137; 103.140. Regulations applicable to "dealers in precious metals, precious stones or jewels" are of limited application and generally exempt retail businesses. *See* 31 C.F.R. 103.140. In regard to insurance companies, only those companies that are engaged within the United States as a business in the issuing of a permanent life insurance policy (other than group policies), annuity contracts (other than group contracts) and "any other insurance product with features of cash value or investment" are required to implement anti-money laundering programs. *See* 31 C.F.R. 103.137.

[33] 31 C.F.R. 103.170. These include businesses such as: agencies of federal, state or local government carrying out a duty or power described in the definition of "financial institution;" loan or finance companies; travel agencies; telegraph companies; sellers of automobiles, airplanes and boats; persons involved in real estate closings or settlements; private bankers; commodity pool operators; commodity trading advisors; and investment companies; some insurance companies; and some dealers in precious metals, stones or jewels. However, *proposed* regulations have been published for "Unregistered Investment Companies" (*see,* 67 Federal Register, 60617, Thursday, September 26, 2002) and a regulatory scheme for "persons involved in real estate closings or settlements" is apparently under consideration (*see,* 68 Federal Register, 17569, Thursday, April 10, 2003,). No *final* rules have yet been issued for these two categories of "financial institution."

[34] The list of exempted "financial institutions" is found at 31 C.F.R. 103.170.

(i) Anti-Money Laundering Programs: All Anti-Money Laundering Programs must be in writing. The Bank Secrecy Act and the implementing regulations further require that institutions subject to implementing such Programs must also: (i) formally appoint an Anti-Money Laundering Compliance Officer who is in overall charge of the Program; (ii) the periodic training of appropriate employees about the institution's anti-money laundering policies and procedures; and (iii) the periodic independent audit of the Anti-Money Laundering Program to ensure it has been implemented and is being followed.[35]

Anti-Money Laundering Programs must be "risk based." This means that each institution must carefully consider its customer base, products, services, geographic areas of operation and market area in order to determine the degree of money laundering risk the institution faces, and degree of risk associated with each of these various categories. As a practical matter, this involves the preparation of a written "Risk Assessment" covering each of the factors just noted. Then, based upon that assessment, the institution must develop written policies and procedures specifically designed to address the degree of risk and detect, deter and report money laundering or terrorist financing activity.

(ii) Customer Identification Programs (or "CIP") is required only for some "financial institutions." These include banks, savings associations, credit unions, securities broker dealers, futures commission merchants and introducing brokers, mutual funds and "money services businesses."[36] The Program must be in writing and, if the institution is also required to have an anti-money laundering program, it must be included as part of that program. CIP must include, at a minimum, procedures to verify the name, date of birth, address or principal place of business and identification number. Verification may be done through documents specifically set forth in the Program (generally, a government-issued photo identification for persons, or documents showing the legal existence of an entity). Verification may be made through non-documentary procedures, but the specific procedures must be specified in the Program. The Program must also prescribe the procedures to be followed by the institution when verification cannot be accomplished, including the circumstances under which an account must be closed for lack of verification. The institution must maintain copies of all records and documents used in the verification process.

(iii) Reporting of "Suspicious Transactions": *Some* "financial institutions are required to report in writing "suspicious transactions" to the Treasury Department (specifically, to the Financial Crimes Enforcement Network, or "FinCEN"). The "financial institutions" subject to this requirement are: (i) banks;[37] (ii) mutual funds; (iii) insurance companies covered under 31 C.F.R. 103.137; (iv) brokers or dealers in securities; (v) futures commission merchants and introducing brokers in commodities; (vi) "money services businesses;" and (vii) casinos.[38]

---

[35] 31 U.S.C. §5318(h).

[36] *See variously,* 31 C.F.R. 103. 121 through 123, and 103.131.

[37] "Banks" include all commercial banks, trust companies, savings or building and loan institutions and credit unions organized under federal or state law; private banks; institutions insured under the National Housing Act; savings banks; and foreign banks operating in the United States. 31 C.F.R. 103.11(c).

[38] *See variously,* 31 C.F.R. 103.15 through 103.21.

Generally, transactions are considered to be "suspicious" and subject to the reporting requirement where the institution knows, suspects or has reason to suspect that a transaction: (i) involves funds derived from illegal activities; (ii) is intended or conducted in order to hide or disguise funds or assets derived from illegal activities; (iii) is designed to evade any reporting or other requirements of the Bank Secrecy Act or the BSA regulations; (iv) has no business or apparent lawful purpose; or (v) is not normal for the customer involved, and the institution knows of no reasonable explanation for the transaction.

The Bank Secrecy Act provides a "safe harbor" for "financial institutions" (and their officers, directors, employees and agents) reporting suspicious transactions or activity. No "financial institution" may he held liable to any person or entity under and any federal stature or regulation, or under the constitution, law or regulation of any state or political subdivision, for disclosing suspicious activity or for failing to notify the person or entity who is the subject of or named in the report.[39]

No "financial institution" (or any officer, director, employee or agent) may notify any person or entity involved in the activity or transaction that the transaction or activity has been or is intended to be reported.[40]

The form used for reporting "suspicious transactions" depends upon the type of institution making the report. In all cases, however, the report must be filed within thirty days after the date of the detection of the facts that constitute grounds for filing. Filing may be delayed an additional thirty days in order to enable the institution to identify a suspect, but in no case may filing be delayed more than sixty days. Transactions involving on-going money laundering schemes or terrorist financing must be verbally reported immediately upon suspicion to an appropriate law enforcement agency.

3. Reporting Large Cash Transactions

The unique feature of cash is that it leaves little or no documentary evidentiary trail. Unlike credit card transactions or a check purchases, which leave records identifying the date and nature of the transaction as well as the names of the persons involved, when a person engages in a cash transaction there is rarely any record (other than a personal receipt) of the transaction's occurrence, and a record showing the nature of the transaction or, more importantly, the persons involved in it, is even rarer still. In an effort to overcome the absence of a paper trail in cash transactions, federal laws require virtually all businesses in the United States to file reports with the federal government on all cash transactions over $10,000.

(a) Cash Reporting for Certain "Financial Institutions": Currency Transaction Reports: Section 5313 of the Bank Secrecy Act authorizes the Secretary of the Treasury to require domestic financial institutions to make certain reports regarding the transfer of currency. Pursuant to this authority, the Secretary requires that certain financial institutions must report all

[39] 31 U.S.C. § 5312(g)(3). The "safe harbor" applies to any "financial institution" that makes a "voluntary" disclosure. *Id,* Therefore, the "safe harbor" applies even to *all* "financial institutions," including those that are not *required* by regulation to make such reports.

[40] 31 U.S.C. § 5318(g)(2).

cash transactions in excess of $10,000 which occur within a single business day by or on behalf of the same person.[41] Cash transactions are those involving the coin or paper money of the United States, as well as foreign currency.[42]

Reports must be made within fifteen days of the transaction to the Internal Revenue Service on a "Currency Transaction Report" ("CTR") or FinCEN Form 104.[43] A reportable cash transaction includes the aggregate of multiple cash transactions conducted at all of a reporting institution's branches and agencies on a single day if the transactions are conducted by or on behalf of the same person or entity.

It is illegal to intentionally fail to file a CTR, or to intentionally file one that is inaccurate or purposely omits required information. Violations are punishable as violations of the Bank Secrecy Act.

The financial institutions required to report such transactions on Currency Transaction Reports include depository institutions such as banks, credit unions and thrift institutions, broker dealers in securities, commodities futures traders, "money services businesses (that is, currency dealers or exchangers; check cashers; issuers or sellers of cashier's checks, traveler's checks, money orders, or stored value; and money transmitters), and casinos and card clubs.[44]

(**b) Cash Reporting for Other Businesses: IRS Form 8300:** Section 5331 of the Bank Secrecy act and section 6050I of Title 26, United States Code, require that any person who is engaged in a trade or business and who, in the course of such trade or business, receives more than $10,000 in cash in one transaction, or in two or more "related" transactions, is required to file a report of the transaction with FinCEN and the Internal Revenue Service. This requirement includes *all other* "financial institutions" not otherwise required to file CTRs, as well as *all other* persons and businesses in the United States, if they receive over $10,000 "cash" in the course of their trade or business.[45] Although required by two separate statutes, reports are made on a single form, an IRS/FinCEN Form 8300, which is transmitted to the IRS.

It is illegal to intentionally fail to file a Form 8300, or to intentionally file one that is inaccurate or purposely omits required information. Violations are punishable by civil fines of up to $100,000, or criminally by imprisonment up to ten years and a fine of up to $500,000.

In addition to reporting "cash" transactions, every business must furnish a single, annual written statement to each person named on a Form 8300 which includes the name and address of the business, the total amount of cash reported to have been received in the calendar year from or on behalf of the person named in the Form, and a statement saying that the information was reported

---

[41] 31 C.F.R. 103.22.

[42] 31 C.F.R. 103.11(h).

[43] Casinos are required to use FinCEN Form 103. Casinos located in Nevada are required to use FinCEN Form 103-N.

[44] Reporting for certain customers may be exempted under the Treasury Department regulations. *See,* 31 C.F.R. 103.22(d).

[45] 31 C.F.R. 103.30.

to the IRS. The statement must be sent to each person named in the Form on or before January 31 of the year following the calendar year in which the cash was received.[46]

(i) What Constitutes "Cash": Reports are made on an IRS Form 8300. Like Currency Transaction Reports, "cash" includes not just U.S. currency, but also the currency of any other country. Unlike Currency Transaction Reports, however, "cash" is not limited just to currency. It also includes "monetary instruments," which are defined as cashier's checks (by whatever name called, including "treasurer's checks" and "bank checks"), bank draft, traveler's checks or money order *with a face value of under $10,000.*[47]

(ii) Reportable Transactions: The law requires that if the Company receives more that $10,000 in cash in one transaction or in two or more "related" transactions, it is required to file a Form 8300 with the Internal Revenue Service. A “transaction” means the underlying event precipitating the payer's transfer of currency to the recipient. This includes, but is not limited to, the sale of goods or services, the sale of real property, the sale of intangible property, the rental of real or personal property, the exchange of currency for other currency, the establishment or maintenance of a custodial, trust or escrow arrangement, the payment of a pre-existing debt, the conversion of currency into a negotiable instrument, the reimbursement for expenses paid, or the making or repayment of a loan.[48]

Any transactions between a business and the same customer which occur within a twenty-four hour period are considered to be one transaction for reporting purposes. A Form 8300 must be filed within fifteen (15) days of the receipt of over $10,000 cash.

(iii) "Related" Transactions: Transactions are considered "related" for cash reporting purposes even if they occur over a period of more than 24 hours, if the receiving business knows or has reason to know that each transaction is one of a series of connected transactions.[49]

For example, a customer intends to purchase a $45,000 product from a business and pay over a five month period. The $45,000 is a single transaction for cash reporting purposes. Therefore, if the customer pays $9,000 each month for five months, if any part of any of the payments are made in cash, once the cash portions total over $10,000 a Form 8300 must be filed on the cash payments. Thus, if the first $9,000 payment is by personal check, the transaction is not reportable because a personal check is not cash. If the second payment is $9,000 in cash, it is not reportable because the amount of cash received by the Company is under $10,000. If the third payment is by cashier's check for $9,000, a Form 8300 must be filed because the business has now received, in one transaction over $10,000 in cash -- $9,000 in currency and $9,000 in a cashier's check (a "monetary instrument" which is the equivalent of cash). If the fourth payment is $9,000 cash, a Form 8300 does not have to be filed because, after filing the first Form 8300, the $10,000 count starts over again. If, however, the fifth payment is $9,000 in a traveler's check (again, the "monetary instrument" equivalent of cash), a second Form 8300 must be filed because

[46] 26 C.F.R. 1.6050I-1(f).

[47] 31 C.F.R. 103.30(c)(1); 26 C.F.R. 1.6050(c)(ii)(B).

[48] 31 C.F.R. 103.30(c)(12)(i).

[49] 31 C.F.R. 103.30(c)(12(ii).

the business has again received, in one transaction (the original $45,000 transaction) over $10,000 in cash -- $9,000 in currency and $9,000 in the traveler's check.

(iv) Multiple Payments: The receipt of cash deposits or cash installment payments for a single transaction are reported differently, depending on the amounts of cash paid in the initial and subsequent payments.

If a customer's initial payment in one transaction is over $10,000 cash, that payment must be reported on Form 8300 within 15 days of the transaction. If the initial payment is in cash but does not exceed $10,000, then the initial payment must be combined with subsequent cash payments made within one year. As soon as the total of cash payments on the transaction exceeds $10,000, a Form 8300 must be filed. If more cash payments on that transaction are later received within the one year period, they must be separately reported every time they total over $10,000.

Returning to the $45,000 hypothetical purchase, if the customer pays $9,000 each month for five months, if any part of any of the payments are made in cash, once the cash portions total over $10,000 a Form 8300 must be filed on the cash payments. For example, if the first $9,000 payment is by personal check, the transaction is not reportable because a personal check is not cash. If the second payment is $9,000 in cash, it is not reportable because the amount of cash received by the Company is under $10,000. If the third payment is by cashier's check for $9,000, a Form 8300 must be filed because the Company has received, in one transaction (the necklace purchase) over $10,000 in cash -- $9,000 in currency and $9,000 in a cashier's check (the equivalent of cash). If the fourth payment is $9,000 cash, a Form 8300 does not have to be filed because, after filing the first Form 8300, the count starts over again. If, however, the fifth payment is $9,000 in a traveler's check (the equivalent of cash), a second Form 8300 must be filed because the Company has again received, in one transaction (the necklace purchase) over $10,000 in cash -- $9,000 in currency and $9,000 in the traveler's check.

(c) "Bulk Cash Smuggling": Any person who physically transports, mails, ships, or causes the same, of any currency or "monetary instrument" in an aggregate amount of over $10,000 into or our of the United States must report it to the U.S. Customs Service. The report must be made on a "Report of International Transportation of Currency or Monetary Instruments," also known as a "CMIR" or FinCEN Form 105.[50]

The knowing and intentional failure to file the report the international movement of cash or monetary instruments in excess of $10,000 may result in the seizure and civil or criminal forfeiture of the currency and monetary instruments being transported. If the currency or monetary instrument is concealed for the purpose of avoiding a report, the container or conveyance carrying the funds may also be seized. A knowing and intentional failure to report can be also punished criminally by imprisonment for up to five years.[51]

The report must be filed before or at the time of the entry or departure into or from the United States. It may also be made by mail on or before the date of entry, departure, mailing or

[50] 31 C.F.R. 103.23(a).

[51] 31 U.S.C. § 5332.

shipping. However, as a practical matter, the report should be filed directly with U.S. Customs at the time or entry or departure.

A person *receiving* cash or monetary instruments from outside the United States must file a FinCEN Form 105 within fifteen days of receipt if the Form has not already been filed by the person sending or causing the sending of the funds[52]

For purposes of this law, "currency" means the coin or paper money of the United States, as well as the coin or paper money of a foreign country. Thus, the import or export of foreign currency whose value in U.S. dollars exceeds $10,000 must be reported. The term "monetary instrument" means: traveler's checks in any form; all forms of negotiable instruments (including personal and business checks) that are either in bearer form, that may be endorsed without restriction, that are made out to a fictitious payee, or that are in any other form such that title passes upon delivery; incomplete instruments which are signed but with the payee's name left out; and securities or stocks in bearer form or whose title passes on delivery.[53]

There are a number of *exceptions* to this reporting requirement, including:

(i) Banks, foreign banks, and securities broker dealers shipping by mail or by common carrier;

(ii) Certain overland shipments by a domestic commercial bank or trust company for an established customer;

(iii) Common carriers of passengers with respect to funds carried by passengers;

(iv) Common carriers of goods with respect to funds shipments not declared to the common carrier;

(v) A non-U.S. citizen or resident for funds mailed or shipped from abroad to a bank or broker dealer by mail or common carrier;

(vi) Issuers of traveler's checks.[54]

(d) "Structuring": In order to avoid the large cash transaction reporting requirements, money launderers and terrorists frequently attempt to disguise one single cash transaction over $10,000 as multiple, separate transactions, each under $10,000. This type of activity, when designed to avoid the filing of any of the large cash transaction reporting forms, is called "structuring." When done for the purpose of avoiding the filing of required large cash transaction reporting forms is illegal and is punishable by criminal prosecution and imprisonment up to five years. Such violations, if committed while violating another law of the United States

[52] 31 C.F.R. 103.23(b).

[53] 31 C.F.R. 103.11(u).

[54] 31 C.F.R. 103.23(c). However, all exempted persons would be well advised to file the FinCEN Form 105 regardless of any supposed exemption, in order to avoid erroneous seizures by U.S. Customs officials.

or as part of a pattern of any illegal activity involving over $100,000 in a one year period are punishable by a fine of up to $500,000 and imprisonment for up to ten years.[55]

4. Transactions With Prohibited Persons, Groups, Entities and Countries: A number of federal laws impose severe restrictions and sanctions against various persons, groups, entities and countries considered to be terrorists, supporters or terrorist activity, or illegal narcotics "kingpins." These sanctions are implemented through regulations issued by the U.S. Treasury Department, Office of Foreign Assets Control ("OFAC") and apply to all "United States Persons."

Generally, a "United States Person" includes a national of the U.S. anywhere in the world, any resident alien, any person within the U.S., any entity composed principally of nationals or permanent resident aliens of the U.S., or any corporation organized under the laws of the U.S., any state, the District of Columbia, or any territory or possession of the U.S. Generally, for anti-money laundering and anti-terrorist financing purposes, the term does not include foreign subsidiaries of U.S. entities. However, the term *does* include, and the prohibitions *do* directly apply to, individual "United States Persons" located anywhere in the world, regardless of by whom they are employed.[56]

OFAC maintains a list foreign the persons, groups, entities and countries deemed to be supporters of terrorist activity, terrorists, of international narcotics "kingpins" subject to the sanctions. This is generally known as the "OFAC List" or the "SDN List" (SDN stands for "Specially Designated National").

Generally, the OFAC regulations prohibit any United States Person from engaging in any transaction or transfer of any funds or property of whatever with a SDN. They further generally require that all property and assets of "SDNs" be either "blocked" (that is, placed in an interest bearing account not accessible by the SDN), or that any transaction involving any property or funds belonging to a SDN rejected, and promptly reported to OFAC. However, the precise prohibitions imposed by OFAC regulations against SDNs, and the specific requirements imposed on United States Persons, vary according to the particular reason for including the person, group, entity or country on the OFAC List. The OFAC regulations, which are voluminous, are generally found at 31 C.F.R. 500 through 598.[57] Since the specific sanctions, prohibitions and requirements imposed by OFAC regulations vary according to the reason a person, group, entity or country has been placed on the list, the names found on the List also refer to the particular reason for inclusion. It is thus important not only to identify SDNs, but also to know their specific designation in order to know the precise requirements and prohibitions imposed on United States Persons by the regulations.

---

[55] 31 U.S.C. § 5324.

[56] *See generally,* 18 U.S.C. § 3077(2). However, the specific OFAC regulations should be checked for the precise application of the OFAC regulations, as they may be different depending upon the sanction program involved.

[57] A useful reference for finding the specific regulatory prohibitions and requirements for specific sanctions programs can be found at 31 C.F.R. 500, Appendix A to Chapter V, located immediately following 31 C.F.R. 598.

As a general rule, it is illegal to conduct any business transaction, facilitate any business transaction, or provide any service to any person, group or organization on the OFAC List. Violations can be punished by severe fines and imprisonment, depending upon the statute and sanctions program involved, but civil fines imposed by OFAC against United States Persons violating OFAC regulations can be substantial, frequently involving hundreds of thousands of dollars and, in some cases, millions.

5. Special Rules for "Money Services Businesses": In addition to maintaining formal Anti-Money Laundering Programs and reporting "suspicious transactions," all "money services businesses are required to register with FinCEN.[58] Failure to register is a federal felony punishable by fine and imprisonment for up to five years.[59]

In addition, many *states* also require money services businesses to register. Failure to register with a state, if required is required by state law, is a federal felony.[60] It is, therefore, essential for every such business to not only comply with the federal registration regulations, but also to check the laws of each state in which it does business. In some cases, a money services business may have to file multiple registrations. Care must be taken to closely examine the definition of the term "money services business" under both the federal regulations and local state law, because they frequently differ. This can result in a business having to register in some states but not others, or with FinCEN but not with the state, or with the state but not with FinCEN.

Agents and branches of money services businesses are not required by federal regulation to register with FinCEN, although the business must report information about its branch locations or offices, and must maintain a list of its agents. This list must include each agent's name, address, telephone number, type of service provided by the agent, the agent's bank, the year the agent first became an agent, the number of branches or sub-agents the agent has, and a listing of the months in the preceding twelve months in which the agent's gross transaction amount exceeded $100,000.[61]

Registration is valid for a two-year period and a copy of the registration must be kept at a location in the United States for five years. If, however, the business is subject to a state registration requirement, then a change in control which requires re-registration with the state requires re-registration with FinCEN. In addition, the federal regulations also require re-registration with FinCEN if there is a transfer of more that ten per-cent of the voting power or equity interest of the business. Further, if the business experiences a more than fifty per-cent increase in the number of its agents during any registration period, the business must re-register with FinCEN. Re-registration must be done within 180 days of the event triggering the re-registration requirement.[62]

---

[58] 31 C.F.R. 103.41(a).

[59] 18 U.S.C. § 1960(a).

[60] 18 U.S.C. § 1960(b).

[61] 31 C.F.R. 103.41(d).

[62] 31 C.F.R. 103.41(b).

4. SHOULD MY COMPANY CARE ABOUT AN ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM?

Any business that is a "financial institution" under the Bank Secrecy Act and which is required to implement an Anti-Money Laundering Compliance Program *must* care, because failure to implement the Program could expose the business to criminal, civil and administrative penalties.[63] For such businesses, it is equally important to monitor changes in or additions to that requirement (for example, a requirement to report "suspicious transactions" or maintain certain types of records may be added to an already-existing Compliance Program requirement). Failure to comply with the applicable Treasury regulations can be punished both civilly and criminally under the Bank Secrecy Act, and may also subject regulated "financial institutions" to severe administrative penalties imposed by their federal regulatory agency for failure to comply, or even for failure to fully and sufficiently comply.

Any other business that is a "financial institution" under the Bank Secrecy Act should closely monitor the Federal Register in order to determine whether the Treasury Department intends to issues regulations removing it from the exemption in 31 C.F.R. 103.170. In such cases, Treasury normally will issue a Notice of Proposed Rule Making in the Federal Register, explaining and stating the proposed regulations and inviting public comment. A Notice of Proposed Rule Making is a clear indication that an exempted "financial institution's" status is about to change, although a substantial amount of time may elapse before a *Proposed* Rules made a *Final* Rule.

Further, for all businesses, the best defense against becoming unwittingly involved in a possible violation of the Money Laundering Control Act is to have an effective Anti-Money Laundering Compliance Program. Such a Program can be used to demonstrate that the business is a "good corporate citizen" that took reasonable steps to avoid involvement (through willful blindness or otherwise) in criminal money laundering activity.

Finally, the senior management of every corporation, regardless of whether it is a Bank Secrecy Act "financial institution," arguably has a duty to include anti-money laundering policies and procedures as part of the overall compliance program which the Delaware Chancery Court, in the leading *Caremark* decision, has held that corporate management is duty-bound to have under Delaware law in light of the Sentencing Guidelines.[64]

5. WHAT ARE THE ELEMENTS OF AN EFFECTIVE ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM?

As noted in Section 3.3(c) above, the minimal requirements for a *mandatory* Anti-Money Laundering Program are: (i) the Program must be in writing; (ii) the Program must have a formally appointed Anti-Money Laundering Compliance Officer; (ii) periodic training of

[63] Businesses required to implement AML Programs are listed in Section 3.2(b) at p. 10, above.

[64] *In re Caremark Int'l Inc. Derivative Lit.*, 698 A.2d 959, 970 (Del. Ch. 1996).

appropriate employees about the institution's anti-money laundering policies and procedures; and (iv) the periodic independent audit of the implemented and is being followed.[65]

Anti-Money Laundering Programs must be "risk based." This means that each institution must Anti-Money Laundering Program to ensure it has been carefully consider its customer base, products and market in order to determine the degree of money laundering risk the institution faces. As a practical matter, this involves the preparation of a written "Risk Assessment" covering each of the factors just noted. Then, based upon that assessment, the institution must develop written policies and procedures. Those policies and procedures must be specifically designed to address the degree of risk to which the business is exposed, and to then detect, deter and report money laundering or terrorist financing activity based upon that risk level.

A key element for the prevention and detection of money laundering and terrorist financing is to develop effective "Know Your Customer" procedures. In every transaction, each business should be diligent in knowing who it is dealing with, and have reasonable grounds to believe that each customer is entirely legitimate. This includes confirming an individual customer's true identity and, for customers that are businesses, ensuring that every entity with which one does business is, in fact, a legally established entity.

For individual customers, this normally means verifying identity through a government-issued photo identification, and in appropriate cases determining the customer's source of funds or wealth. For business customers, it normally means securing a copy of articles of incorporation, government-issued licenses, government tax identification numbers, trust documents, partnership registrations or the like. It can also include procedures to verify business information by telephone or through publicly available information. For some businesses, it is neither possible nor practical, from a cost or customer relations point of view, to secure such documentation for *every* customer. This is where the risk assessment comes into play. Depending upon the degree and type of risk, a business should determine when to require identification, what type of identification to secure, and what follow-up procedures are appropriate. The point to keep in mind is that, depending on the degree of risk and the volume of business being done, each business should attempt to establish, as effectively and efficiently as it can, that the individual or business it is doing business with is who it claims to be, is engaged in legitimate business activities, is using funds derived from legitimate business legitimate or sources of wealth and income.

(i) The Anti-Money Laundering Compliance Officer: The Compliance Officer should be appointed by the Board of Directors or Senior Management. The actual title is not important, although the Compliance Officer must have a level of authority and responsibility in the company sufficient to implement, supervise and enforce the Compliance Program on a daily basis, and sufficient resources (budgetary and personnel) to perform his or her function.

The Compliance Officer must be a qualified person who is knowledgeable about money laundering and the Money Laundering Control Act. For "financial institutions," it is critical that

[65] 31 U.S.C. §5318(h). For "financial institutions" *required* to have such Programs, essential elements may also include Customer Identification Programs and procedures for identifying and reporting "suspicious transactions."

the Compliance Officer be fully knowledgeable about the Bank Secrecy Act and the implementing regulations that apply to the particular business. The Compliance Officer should also have a full knowledge of the business, its products, services, operations, general customer base and money laundering risk assessment.

Finally, it is imperative that the Compliance Officer be of the highest integrity. Bad actors must be kept out of the position, and out of the overall supervision and operation of the Compliance Program. The Board and Senior Management must take reasonable steps to screen out persons whom the company knows, or should know through the exercise of due diligence, have a history of engaging in illegal activity or other misconduct;

(ii) Employee Training: For all Bank Secrecy Act "financial institutions" that are required to maintain Anti-Money Laundering Programs, periodic employee training is mandatory. Periodic employee training is necessary for any other business with an Anti-Money Laundering Compliance Program, because the failure to conduct periodic training will render the Program ineffective.

All appropriate employees should be trained on money laundering in general and on the company's anti-money laundering policies and procedures. Who the "appropriate" employees are will vary from business to business and also depend on the company's risk assessment, but at a minimum should include all employees whose duties could expose them to money laundering. Generally this will include management, sales, finance and accounting personnel. Training should be tailored to the person's specific responsibilities. In addition, new staff should be given an overview of the Compliance Program during employee orientation. For "financial institutions," it is critical that employees be trained about the Bank Secrecy Act and the implementing regulations that apply to the particular business.

Training should be periodic (generally, annually) and include not only training on basic policies and procedures, but also current anti-money laundering developments and changes to any company policies and procedures. Important developments and changes should be disseminated on an ongoing basis, as needed.

The company should document its training program and keep accurate records of the dates of the periodic employee training, the content of the training, training and testing materials, and attendance records.

(iii) Independent Audit: An Anti-Money Laundering Compliance program should be periodically tested independently to ensure it has been implemented, followed and enforced. For all Bank Secrecy Act "financial institutions" that are required to maintain Anti-Money Laundering Programs, periodic independent auditing of the Program is mandatory.

While the frequency of the independent audit is not prescribed, even for "financial institutions," it is generally a sound practice to conduct independent testing annually.

The periodic audit must be "independent" in the sense that it is conducted by persons who are not involved in or responsible for the Program's operation. Thus, it may be conducted by the internal audit department, outside auditors, consultants or other qualified persons.

The persons conducting the independent audit should be knowledgeable about the Program, the policies and procedures included in the Program, the business and its operations, and the company's money laundering risk assessment. For all Bank Secrecy Act "financial institutions" that are required to maintain Anti-Money Laundering Programs, they should also be knowledgeable about the Bank Secrecy Act and the regulations applicable to the company. They audit should also be familiar with the company's money laundering risk assessment, because the audit should be "risk based" and evaluate the quality of risk management for all operations and departments involved in applying the Program's policies and procedures.

The persons conducting the independent audit should report directly to the company board of directors or a designated board committee. Deficiencies and corrective recommendations should then be conveyed to senior management and the Compliance Officer for correction and follow-up. Senior management should ensure, through the Compliance Officer, that identified deficiencies are promptly addressed and corrective recommendations implemented.

6. WHAT ROLE DOES TOP MANAGEMENT HAVE IN ADMINISTERING AN ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM?

The success of any compliance program depends upon the support and involvement of top management. Not surprisingly, the Treasury Department regulations requiring certain "financial institutions" to implement Anti-Money Laundering Programs thus expect the company's board of directors and senior management to issue the policies and procedures designed to implement the Compliance Program itself, as well as those designed to deter and detect money laundering. Top management is also expected to monitor, at least through the periodic independent audit, the operation of the Program. While clearly not applicable to all businesses, the regulations establish a basic standard for the role of top management.

In addition to establishing the Program and issuing the appropriate policies and procedures, the board of directors, or at least the senior management, should appoint the Compliance Officer. The Compliance Officer should report directly to senior management and the board.

It is the duty of the board and senior management to ensure that the Compliance Officer is qualified, and that he or she has the necessary resources (in terms of budget and staff) to perform the assigned duties. The board and senior management need to understand the content and operation of the Compliance Program and exercise reasonable oversight with respect to its implementation and effectiveness. The board and senior management should thus generally supervise the Compliance Officer, and receive periodic reports from him or her concerning the operation of the Compliance Program and any updates or changes needed in company policies and procedures. The individual delegated day-to-day operational responsibility should report periodically to senior management and shall have direct access to the board of directors.

7. WHO SHOULD ADMINISTER THE ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM?

Several different departments within the company may have significant roles to play in the day-to-day operation of the Compliance Program, including the company audit or accounting department, the security department, human resources, and the legal department. However, their

various compliance efforts must be coordinated as part of a single program, so the Compliance Officer should be responsible and accountable for overseeing the company's compliance efforts. Again, in order to accomplish this task and ensure the smooth and effective operation of the Compliance Program, the Compliance Officer needs to have sufficient line authority and resources.

8. WHAT ARE THE ACTUAL STEPS A COMPANY MUST TAKE TO CREATE AN EFFECTIVE ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM?

The regulations provide no guidance on *how* to create an effective Anti-Money Laundering Program. Reference to the United States Sentencing Guidelines, however, provide some direction that, at a minimum, a company should take:[66]

(1) Establish policies, standards and procedures to prevent and detect money laundering;

(2) Conduct a risk assessment based on the company's products, services, customer base and geographic location(s), and develop specific risk-based procedures to meet the perceived risk areas. A risk assessment is *not* a one-time-only exercise. It is a continuing process that continually takes into account changes in methods of money laundering, new products or services offered by the company, changes in the company's customer base and geographic areas of operation, and changes in the law or applicable regulations;

(2) Ensure that the company's Board of Directors and Senior Management understand the content and operation of the Compliance Program and exercise reasonable oversight with respect to its implementation and effectiveness. Specific senior manager(s) should have overall responsibility to ensure the implementation and effectiveness of the Program. A Compliance Officer should be delegated at the outset to conduct or supervise the risk assessment, develop appropriate procedures, and oversee the drafting, implementation and day-to-day operation of the Program. This person should be afforded adequate resources and authority to accomplish these tasks.

(3) Take reasonable steps to ensure that the Compliance Officer and his or her staff are adequately knowledgeable about the business, money laundering and applicable statutes and regulations. Also ensure that the Compliance Officer and his or her staff are of the highest integrity by screening out persons whom the company knows, or should know through the exercise of due diligence, have a history of engaging in illegal activity or other misconduct;

[66] USSG § 8B.

(4) Take reasonable steps to communicate periodically and in a practical manner the company's its standards and procedures to all officers, employees and, as appropriate, its agents, through effective training programs and otherwise disseminating information;

(5) Take reasonable steps to (a) ensure that the program is followed, including using monitoring and auditing to detect criminal conduct; (b) evaluate periodically the program's effectiveness; and (c) have a system whereby employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation (although a mechanism for anonymous reporting is not required);

(6) Promote and enforce the program through appropriate incentives and disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct; and

(7) Take reasonable steps to respond appropriately to money laundering by customers and to prevent further similar conduct, including making any necessary modifications to the compliance and ethics program.[67]

9. IS THERE A STANDARD ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM THAT MY COMPANY CAN EFFECTIVELY USE?

There is no such thing as a "one size fits all" anti-money laundering compliance program. An effective program must be based on a risk assessment that is specific to each company. Each company must examine the nature of its business, its products and services, its customer base and the areas in which it operates in order to determine its potential exposure to money laundering, and the policies and procedures it adopts must be designed based on that company-specific analysis. Each company must prioritize the risks that it faces in terms of the degree of money laundering risk associated with its products, services, locations and customers.

4464822_v1

67 USSG § 8B2.1(b).